UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/758,242	01/12/2001	Prabir Bhattacharya	9432-000128	7867

7590 08/25/2004

Harness, Dickey & Pierce, P.L.C.
P. O. Box 828
Bloomfield Hills, MI 48303

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/758,242	BHATTACHARYA ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on January 12, 2001. Claims 1 – 20 were received for consideration. No preliminary amendments for the claims were filed. Claims 1- 20 are currently under consideration.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 7 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 7 is dependent on claim 6, which recites the limitation "encrypting the secondary keys with the master key." Claim 7 contains the limitation "encrypting subsequent secondary keys in the set with all preceding secondary keys in the set." This would result in the secondary keys being encrypted with keys that are already encrypted by the master key by virtue of the limitation of claim 6.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 11 – 13 are rejected under 35 U.S.C. 102(b) as being anticipated by Hirose (U.S. Patent 5,917,915).

Regarding claim 11, Hirose discloses:

A method for enabling a device to access an encrypted data file content, the method comprising the steps of:

decrypting single-encrypted blocks of the data file with a master key (column 3 lines 1 – 14);

decrypting dual-encrypted blocks of the data file with the master key and a secondary key (column 3 lines 1 – 14); and

repeating the decryption steps for a set of secondary keys such that the device is able to access the data file content once for each secondary key in the set (column 3 lines 1 – 14).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Hirose discloses:

The method of claim 11 further including the step of decrypting the blocks on a block-by-block basis such that the device only has access to the data file content one block at a time (column 3 lines 1 – 14).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Hirose discloses:

The method of claim 12 further including the step of re-encrypting the single-encrypted blocks with a new master key (column 2 line 60 – column 3 line 2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1 – 5 and 8 - 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirose (U.S. Patent 5,917,915) in view of Watts (U.S. Patent 6,587,842).

Regarding claim 1, Hirose discloses:

A method for encrypting a data file content, the method comprising the steps of: encrypting the data file with a master key (column 2 line 60 – column 3 line 14); and generating one or more dual-encrypted blocks based on a set of secondary keys, the dual-encrypted blocks contained within the encrypted data file (column 2 line 60 – column 3 line 14).

Hirose does not explicitly describe providing the encrypted data file and an attachment file to an authorized user, the attachment file enabling a device to access the data file content once for each secondary key. Watts teaches a system where an electronic message (e-mail) is transmitted to a customer along with an attachment "key-file" which has the keys necessary to access the encrypted data (Figure 2, column 4 lines 37 – 47). In the method of Hirose, the multiple encrypted data is sent over a network to a receiver which must possess multiple keys to decrypt the multiple encrypted data. Hirose does not explicitly disclose the method of distributing the unique keys to the receiver, but Hirose reveals that two different keys would be required to decrypt a twice encrypted data (column 3 lines 5 – 15) and that the data is transported over any type of data network (column 2 lines 49 – 67). It was well-known at the time of invention that e-mails with attachment files are a common way to send data files to users. Hirose also discloses the preferred embodiment of the invention is to have multiple secondary keys which correspond to different types of data. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to each type of data with its corresponding key in an attachment file so that the data file could

be decrypted on the receiver end without having one standard key to decrypt all types of data.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Hirose discloses:

The method of claim 1 further including the steps of:

randomly generating the master key (column 2 lines 60 – 67).

Hirose does not explicitly disclose hiding the master key within a data structure of the attachment file. Watts teaches hiding the key in the attachment file (Figure 6, column 5 lines 12 – 26). According to Watts, this hiding of the key makes it "extremely difficult to locate key information" (Figure 6). The hiding of the key makes the transmission of the keys more secure and makes the compromising of the key and the encrypted data difficult. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to hide the key data within the attachment file to make the location of the key information extremely difficult.

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Hirose disclose:

The method of claim 1 further including the steps of:

selecting one or more continuous blocks to be dual-encrypted (column 2 line 60 – column 3 line 15);

randomly generating the secondary keys (column 2 line 60 – column 3 line 15);

generating a duplicate selected block for each secondary key in the set (column 2 line 60 – column 3 line 15);

generating dual-encrypted blocks based on the duplicate selected blocks and the secondary keys (column 2 line 60 – column 3 line 15); and

inserting the dual-encrypted blocks into the data file (column 2 line 60 – column 3 line 15).

Claim 8 is rejected as applied above in rejecting claim 1. Hirose does not explicitly disclose receiving an email message from the attachment file and determining whether another message having the same status content has already been received. Watts teaches a system where an electronic message (e-mail) is transmitted to a customer along with an attachment "key-file" which has the keys necessary to access the encrypted data (Figure 2, column 4 lines 37 – 47). In the method of Hirose, the multiple encrypted data is sent over a network to a receiver which must possess multiple keys to decrypt the multiple encrypted data. Hirose does not explicitly disclose the method of distributing the unique keys to the receiver, but Hirose reveals that two different keys would be required to decrypt a twice encrypted data (column 3 lines 5 – 15) and that the data is transported over any type of data network (column 2 lines 49 – 67). It was well-known at the time of invention that e-mails with attachment files are a common way to send data files to users. Hirose also discloses the preferred embodiment of the invention is to have multiple secondary keys which correspond to different types of data, which would have to be identified for each different data type. Therefore it would have

been obvious to one of ordinary skill in the art at the time the applicant's invention was made to each type of data with its corresponding key in an attachment file with status content so that the data file could be decrypted on the receiver end without having one standard key to decrypt all types of data.

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Hirose discloses:

The method of claim 2 further including the steps of:

creating an odd logarithmic bit integer (column 2 lines 60 – 67); and

incrementing the integer by two until a prime number is found (column 2 lines 60 – 67);

said prime number defining the master key (column 2 lines 60 – 67).

Claim 4 is rejected as applied above in rejecting claim 2. Hirose does not explicitly disclose hiding the master key within a data structure of the attachment file using an NP-hard problem. Watts teaches hiding the key in the attachment file (Figure 6, column 5 lines 12 – 26). According to Watts, this hiding of the key makes it "extremely difficult to locate key information" (Figure 6). The hiding of the key can use any algorithm, and it is obvious to use the NP-hard problem algorithm as it was a well-known algorithm at teh time of invention. The hiding of the key makes the transmission of the keys more secure and makes the compromising of the key and the encrypted data difficult. Therefore it would have been obvious to one of ordinary skill in the art at the time the

applicant's invention was made to hide the key data within the attachment file to make the location of the key information extremely difficult.

Claim 9 is rejected as applied above in rejecting claim 8. Hirose does not explicitly state an attachment which has a status content that defines a current operational state and an identifier for the attachment file. Watts teaches a system where an electronic message (e-mail) is transmitted to a customer along with an attachment "key-file" which has the keys necessary to access the encrypted data (Figure 2, column 4 lines 37 – 47). In the method of Hirose, the multiple encrypted data is sent over a network to a receiver which must possess multiple keys to decrypt the multiple encrypted data. Hirose does not explicitly disclose the method of distributing the unique keys to the receiver, but Hirose reveals that two different keys would be required to decrypt a twice encrypted data (column 3 lines 5 – 15) and that the data is transported over any type of data network (column 2 lines 49 – 67). It was well-known at the time of invention that e-mails with attachment files are a common way to send data files to users. Hirose also discloses the preferred embodiment of the invention is to have multiple secondary keys which correspond to different types of data, which would have to be identified for each different data type. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to each type of data with its corresponding key in an attachment file with status content so that the data file could be decrypted on the receiver end without having one standard key to decrypt all types of data.

Claim 10 is rejected as applied in rejecting claim 8. Furthermore, Hirose discloses:

The method of claim 8 further including the step of storing the status content to a data storage medium (Figure 1 item 8).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Hirose discloses:

randomly generating the new master key (column 2 lines 60 – 67).

Hirose does not explicitly disclose hiding the master key within a data structure of the attachment file. Watts teaches hiding the key in the attachment file (Figure 6, column 5 lines 12 – 26). According to Watts, this hiding of the key makes it "extremely difficult to locate key information" (Figure 6). The hiding of the key makes the transmission of the keys more secure and makes the compromising of the key and the encrypted data difficult. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to hide the key data within the attachment file to make the location of the key information extremely difficult.

Claim 18 is rejected as applied above in rejecting claim 11. Hirose does not explicitly disclose the step of transmitting an e-mail message to a provider of the encrypted data file, the message having a status content. Watts teaches a system where an electronic message (e-mail) is transmitted to a customer along with an attachment "key-file" which

has the keys necessary to access the encrypted data (Figure 2, column 4 lines 37 – 47). In the method of Hirose, the multiple encrypted data is sent over a network to a receiver which must possess multiple keys to decrypt the multiple encrypted data. Hirose does not explicitly disclose the method of distributing the unique keys to the receiver, but Hirose reveals that two different keys would be required to decrypt a twice encrypted data (column 3 lines 5 – 15) and that the data is transported over any type of data network (column 2 lines 49 – 67). It was well-known at the time of invention that e-mails with attachment files are a common way to send data files to users. Hirose also discloses the preferred embodiment of the invention is to have multiple secondary keys which correspond to different types of data, which would have to be identified for each different data type. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to each type of data with its corresponding key in an attachment file with status content so that the data file could be decrypted on the receiver end without having one standard key to decrypt all types of data.

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Hirose discloses:

The method of claim 14 further including the steps of:

creating an odd logarithmic bit integer (column 2 lines 60 – 67); and

incrementing the integer by two until a prime number is found (column 2 lines 60 – 67);

said each prime number defining the new master key (column 2 lines 60 – 67).

Claim 16 is rejected as applied above in rejecting claim 14. Hirose does not explicitly disclose hiding the master key within a data structure of the attachment file using an NP-hard problem. Watts teaches hiding the key in the attachment file (Figure 6, column 5 lines 12 – 26). According to Watts, this hiding of the key makes it "extremely difficult to locate key information" (Figure 6). The hiding of the key can use any algorithm, and it is obvious to use the NP-hard problem algorithm as it was a well-known algorithm at teh time of invention. The hiding of the key makes the transmission of the keys more secure and makes the compromising of the key and the encrypted data difficult. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to hide the key data within the attachment file to make the location of the key information extremely difficult.

Claim 17 is rejected as applied above in rejecting claim 12. Furthermore, Hirose discloses:

The method of claim 12 further including the step of discarding the dual-encrypted blocks after decryption with the secondary keys (column 2 line 60 – column 3 line 15).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Hirose discloses:

The method of claim 13 further including the steps of:

randomly generating the new master key (column 2 lines 60 – 67).

Hirose does not explicitly disclose hiding the master key within a data structure of the attachment file. Watts teaches hiding the key in the attachment file (Figure 6, column 5 lines 12 – 26). According to Watts, this hiding of the key makes it "extremely difficult to locate key information" (Figure 6). The hiding of the key makes the transmission of the keys more secure and makes the compromising of the key and the encrypted data difficult. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to hide the key data within the attachment file to make the location of the key information extremely difficult.

5. Claims 19 – 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirose (U.S. Patent 5,917,915) in view Wu et al (U.S. Patent 6,374,363).

Claim 19 is rejected as applied above in rejecting claim 11. Hirose does not explicitly disclose the step of adding footprint files to a host system, the footprint files enabling detection of copying of the encrypted data file. Wu discloses a method of adding footprint files on a host system comprising comparing the footprint files to files to see if the files are the same or different (column 3 line 43 – column 4 line 8). This provides the benefit of discovering if the file already exists, and can detect if a copy was made on the same host system. The detection of copying of the file is another security measure

to discover illegal copying of files, such as the files of Hirose, so that it can be detected and stopped. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to use footprint files to detect the illegal copying of the files of Hirose, and thereby providing another measure to protect the integrity of the data being transmitted.

Claim 20 is rejected as applied above in rejecting claim 11. Hirose does not explicitly disclose the step of adding footprint data to files to a host system.. Wu discloses a method of adding footprint files on a host system comprising comparing the footprint files to files to see if the files are the same or different (column 3 line 43 – column 4 line 8). This provides the benefit of discovering if the file already exists, and can detect if a copy was made on the same host system. The detection of copying of the file is another security measure to discover illegal copying of files, such as the files of Hirose, so that it can be detected and stopped. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to use footprint files to detect the illegal copying of the files of Hirose, and thereby providing another measure to protect the integrity of the data being transmitted.

6. Claims 6 – 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirose (U.S. Patent 5,917,915) in view of Watts (U.S. Patent 6,587,842) in further view of Cane et al. (U.S. Patent 6,754,827).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Hirose discloses:

The method of claim 5 further including the steps of:

formatting the encrypted secondary keys as a data structure (column 2 line 60 – column 3 line 15).

Hirose does not explicitly teach encrypting the secondary keys with the master key. Cane teaches encrypting secondary keys with a master key (Figure 2) before transmitting the key over a network. Cane states that encrypting the secondary keys with the master key allows access control and provides security and higher assurance of data integrity due to the lower probability of compromising the key (column 2 lines 25 – 55). The invention of Hirose transmits the keys and the data file over a data network, such as the Internet, which could be susceptible to interception. It is obvious that that security and integrity are necessary and providing an extra level of security by encrypting the keys would have been obvious to one of ordinary skill in the art at the time of invention to stymie attempts to intercept and decipher the data file.

Claim 7 is rejected as applied above in rejecting claim 6. Hirose does not explicitly teach encrypting the secondary keys with the master key. Cane teaches encrypting secondary keys with a master key (Figure 2) before transmitting the key over a network. Cane states that encrypting the secondary keys with the master key allows access control and provides security and higher assurance of data integrity due to the lower

probability of compromising the key (column 2 lines 25 – 55). The invention of Hirose transmits the keys and the data file over a data network, such as the Internet, which could be susceptible to interception. It is obvious that that security and integrity are necessary and providing an extra level of security by encrypting the keys would have been obvious to one of ordinary skill in the art at the time of invention to stymie attempts to intercept and decipher the data file.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 703-305-8892. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

E. Moise
EMMANUEL L. MOISE
A/U 2136

KA
07/28/2004